[Brandvoice] Evolution des cyberattaques : plus profondes et sophistiquées, elles se cachent dans le hardware

De plus en plus sophistiquées, les attaques informatiques cherchent maintenant à corrompre les couches situées aux niveaux les plus bas d'une infrastructure IT, ce qui les rend à la fois plus efficaces et plus difficiles à détecter. Si les entreprises, sont déjà sensibilisées à la sécurité logicielle, elles sont moins préparées pour répondre aux attaques dans la partie hardware : quels sont les outils à leur disposition pour se protéger davantage ? Présent depuis 50 ans au cœur des architectures matérielles des datacenters du monde entier, Intel nous a apporté de nombreux éléments de réponse.

Focus sur les attaques de « bas niveau »

Dans ce contexte, les entreprises doivent adapter leur stratégie de sécurité. C'est d'ailleurs un paradoxe : même si les organisations sont de plus en sensibilisées à la cybercriminalité, il leur est de plus en plus difficile de se protéger car les risques augmentent et évoluent constamment. L'une des raisons de ces manquements provient du fait que les stratégies de sécurité ont tendance à se focaliser sur les attaques les plus visibles et plus communes: celles situées dans les couches logicielles plus « hautes » du système informatique (OS, applications, documents etc.), pour lesquelles des réponses existent déjà. Le problème sont les attaques beaucoup plus difficiles à détecter au cœur du hardware, explique Claude Chauvet, expert de la sécurité chez Intel en France. « Nous travaillons sur de nombreux aspects de sécurité du Cloud en ajoutant aux briques matérielles l'intelligence nécessaire et les technologies d'auto-évaluation qui vont permettre de s'assurer que quand on a besoin de démarrer une machine virtuelle dans le Cloud, elle sera ouverte sur un serveur de confiance. Cela nécessite qu'Intel ait réfléchi très en amont aux risques auxquels sont soumis les serveurs, afin d'intégrer dès le design des composants la parade aux futures attaques » indique ce dernier.

Hardware : la source de la confiance

En effet le problème des attaques profondes, et notamment la corruption du BIOS ou des firmwares du serveur, est qu'elles sont quasiment indétectables – ou alors, trop tardivement décelées. Il faut apporter une réponse de sécurisation du data centre tout en protégeant les données – sans sacrifier la performance. L'accélération du chiffrement permet déjà de protéger les données lorsqu'elles sont stockées ou lors d'un déplacement sur le réseau, mais l'objectif suivant d'Intel est de les protéger également au moment où elles sont déchiffrées pour que le processeur puisse les traiter (par des technologies de chiffrement de la mémoire vive, ou mieux encore, par des enclaves mémoire (technologie SGX, Software Guard Extensions) qui agissent comme des coffres-forts afin que même sur un serveur déjà attaqué, ces données demeurent inaccessibles aux éventuels malware présents). De nombreuses autres technologies de sécurité ont été ajoutées au

cœur même du silicium pour répondre à d'autres types d'attaque (Intel® TXT, Intel® Security Essentials, Intel® Threat Detection Technology, Transparent Supply Chain). Pour répondre à l'adage selon lequel n'importe quelle solution de sécurité peut être corrompue par la couche située juste en-dessous, Intel a récemment développé une solution innovante de sécurité au cœur du serveur : PFR (Platform Firmware Resilience), qui consiste en l'ajout d'un processeur reprogrammable FPGA (Field Programmable Gate Array), qui est la seule brique matérielle à avoir le droit de démarrer à l'allumage du serveur. « Le rôle exclusif de cette puce est de tester un par un les firmwares des différents composants de la carte mère (SPI, BIOS, BMC, RAID, et même firmware des alimentations) et de valider leur authenticité. Ces différents composants ne pourront démarrer qu'une fois que le FPGA aura déclaré que les firmwares n'ont pas été modifiés et si c'est le cas, une alerte sera lancée pour rétablir le bon firmware depuis une base sécurisée » note Claude Chauvet. Cette stratégie permet d'établir une chaîne de confiance à chaque étape du processus de boot, pour implémenter ce qu'Intel appelle la "platform root of trust", au-dessus de laquelle chacune des briques logicielles (OS, Hyperviseur, Application) pourra s'installer en toute confiance, car construite sur des fondations déjà sécurisées.

Conclusion

Au-delà des solutions logicielles permettant de lutter contre les attaques « de haut niveau », il est donc important de penser également aux technologies déjà mises en place au cœur du silicium afin d'anticiper les risques à venir, et d'éviter que la cybersécurité d'un système ne s'écroule comme un château de cartes à cause d'une attaque dans ses fondations matérielles.

En savoir plus ?

Retrouvez également l'article Réduire le TCO des entreprises avec la mémoire persistante Intel® Optane™